The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
11/08/2016

SUBJECT:
Multiple Vulnerabilities in Microsoft Graphics Component Could Allow for Remote Code Execution (MS16-132)

OVERVIEW:
Multiple vulnerabilities have been discovered in Microsoft Graphics Component, which could allow for remote code execution. These vulnerabilities exist when the Windows font library improperly handles specially crafted embedded fonts. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are reports of CVE-2016-7256 being exploited in the wild.

SYSTEMS AFFECTED:

- Microsoft Windows Vista, 7, 8.1, RT 8.1, 10
- Microsoft Windows Server 2008 and 2008 R2 (Including Server Core Installations)
- Microsoft Windows Server 2012 and 2012 R2 (including Server Core Installations)
- Microsoft Windows Server 2016 (including Server Core Installations)

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Microsoft Graphics Component, the most severe of which could allow for remote code execution. The vulnerabilities are as follows:

- A remote code execution vulnerability exists when the Windows font library improperly handles specially crafted embedded fonts. (CVE-2016-7256)
- A remote code execution vulnerability exists when the Windows Animation Manager improperly handles objects in memory. (CVE-2016-7205)
- A memory corruption vulnerability exists when the Windows Media Foundation improperly handles objects in memory. (CVE-2016-7217)
- An information disclosure vulnerability exists when the ATMFD component improperly discloses the contents of its memory. (CVE-2016-7210)

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:

Microsoft:

https://technet.microsoft.com/library/security/MS16-132

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7205
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7210
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7217
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7256